



King County
Office of Information
Resource Management

Information Technology Governance Standards

Title	Document Code No.
NETWORK INFRASTRUCTURE POLICY	ITG-P-06-03-02
Chief Information Officer Approval	Effective Date.
	6/17/09
Date	6/17/09

1. PURPOSE:

This document establishes the responsibility and authority for ownership, acquisition, and management of the physical components of the County Enterprise Network infrastructure. This infrastructure must support different sets of business needs at diverse locations throughout the county. The goal of this policy is to ensure consistency in the network architecture and to ensure network components meet established technical standards.

2. APPLICABILITY:

This policy applies to all King County Organizations and Workforce Members. It is intended to focus primarily on those Workforce Members who will be responsible for supporting information technology within their respective Organizations.

3. REFERENCES:

- 3.1. Information Technology Policy and Standards Exception Request Process
- 3.2. Internal Network Protocol Standard
- 3.3. Network Configuration Standard
- 3.4. Network Equipment Standard
- 3.5. Network Naming and Numbering Standard
- 3.6. Physical Infrastructure Standard
- 3.7. Wireless Local Area Network Standard

4. DEFINITIONS:

- 4.1. **County Enterprise Network:** The network commonly used to conduct county business that provides transport of data within and between county facilities and other agencies of county government. This definition also refers to the network used to transport data between the county, other government agencies and the Internet. It does not refer to networks built for the sole purpose of meeting special operations needs of county business units which include, but are not limited to process control and supervisory control networks. Nor does it refer to the King County Institutional Network (I-Net) that is required to meet contractual obligations with I-Net customers and the local cable television utility.
- 4.2. **Network Infrastructure Equipment:** Equipment that enables network connections for a facility, group or individual to other points on the County Enterprise Network. This

Network Infrastructure Policy

definition includes LAN switches, routers and wireless access points serving each facility and those used to aggregate and distribute data destined to other parts of the network. It also includes appliances used to control network traffic and secure the network from unauthorized access. The appliances include, but are not limited to; network traffic shapers, network firewalls, VPN concentrators and network intrusion sensors.

- 4.3. **Organization:** Every county office, every officer, every institution, whether educational, correctional or other; and every department, division, board, and commission.
- 4.4. **Workforce Member:** Employees, volunteers, and other persons whose conduct, in the performance of work for King County, is under the direct control of King County, whether or not they are paid by King County. This includes full and part time elected or appointed officials, employees, affiliates, associates, students, volunteers, and staff from third party entities who provide service to King County.

5. POLICIES:

- 5.1. Specification of communications cabling and its distribution within county facilities shall be the responsibility of the Office of Information and Resource Management (OIRM), Network Services and Telecommunications departments. Requests for communications cabling shall be directed to OIRM for review of needs, development of plans, approval of plans, and coordination of installation. A **Physical Infrastructure Standard** shall be maintained also by OIRM Network Services Department that describes current accepted general specifications for cabling, cable termination, cable spaces, distribution frames, their physical surroundings and support systems.
 - 5.1.1. OIRM reserves the right to remove any unauthorized cables, connections, and hardware.
 - 5.1.2. See the **Network Configuration Standard** for MAC address limitations.
- 5.2. All Network Infrastructure Equipment on the County Enterprise Network shall be owned and maintained by OIRM.
- 5.3. Plans for implementing new local area networks (LANs) and plans for expansion of existing LANs shall be reviewed and approved by OIRM prior to implementation.
 - 5.3.1. For isolated, self-contained LANs, it is recommended that new deployments and expansion of existing LANs be reviewed by OIRM.
 - 5.3.2. In the event that the isolated, self-contained LANs require integration into the County Enterprise Network, any inconsistencies shall be corrected by the Organization in question in order to bring it into compliance with the network policy and standards, prior to the integration with the County Enterprise Network.
- 5.4. A list of supported Network Infrastructure Equipment allowed to reside on the County Enterprise Network shall be maintained as described in the **Network Equipment Standard**. Network Infrastructure Equipment to be installed on the County Enterprise Network shall comply with this standard.
- 5.5. Network Infrastructure Equipment shall be configured in accordance with approved templates that shall be maintained in accordance with the **Network Configuration Standard**.

Network Infrastructure Policy

5.5.1. Desktop switches and/or hubs are not allowed.

- 5.6. All wireless local area network (WLAN) equipment attached to the County Enterprise Network shall comply with the **Network Equipment Standard**. In addition, WLAN equipment shall meet technical requirements described in the **Wireless Local Area Network Standard**.
- 5.7. Network protocols used to transport traffic on the County Enterprise Network shall be restricted according to rules described in the **Internal Network Protocol Standard**. The standard describes currently authorized protocols and ways of complying with this policy when use of unauthorized protocols cannot be avoided. All new applications shall comply with this standard.
- 5.8. Network addressing shall be centrally administered by OIRM. Only addressing assigned by OIRM shall be used in configuring equipment for operation on the County Enterprise Network. In addition, an equipment naming convention shall be followed. Standards describing acceptable methods of naming and addressing of Network Infrastructure Equipment, computers, and other network attached devices are described in the **Network Naming and Numbering Standard**.
- 5.8.1. Logical addressing used for devices shall **not** route on the County Enterprise Network.
- 5.8.2. It is recommended that internal addressing for these devices, such as Meta-sans, be coordinated with OIRM.
- 5.8.3. In the event an Organization's device needs to route onto the County Enterprise Network, all inconsistencies shall be changed by the Organization to comply with the **Network Naming and Numbering Standard**, prior to that device becoming part of the County Enterprise Network.

6. EXCEPTIONS:

- 6.1. Any Organization seeking an exception to this policy must follow the Information Technology Policy and Standards Exception Request Process using the Policy and Standards Request form. This form can be found on the Office of Information Resource Management policies and procedures Web page at <http://kcweb.metrokc.gov/oirm/policies.aspx>.

7. RESPONSIBILITIES:

- 7.1. The Chief Information Officer (CIO) is the approval authority for the **Network Infrastructure Policy**.
- 7.2. OIRM Network, Systems, and Operations is the steward of the Network infrastructure and is responsible for providing all transport services across the King County Wide Area Network (KC WAN). As such, OIRM will become the owners of the network policies, standards, and guidelines.
- 7.3. OIRM is responsible for the operations and maintenance of all Network Infrastructure Equipment connected to the King County Enterprise Network. OIRM is not responsible for Network Infrastructure Equipment that operates solely within an Organization **and** OIRM

Network Infrastructure Policy

has previously determined neither connects to, nor affects the operation of the County Enterprise Network.

- 7.4. OIRM is responsible for protecting the integrity of the County Enterprise Network. To meet this responsibility OIRM shall ensure compliance with the terms detailed in the **Network Infrastructure Policy**.
- 7.5. OIRM is responsible for the security of the County Enterprise Network. Policies, standards, guidelines, and associated oversight relating to Network security are established and maintained by the Chief Information Security and Privacy Officer (CISPO).
- 7.6. Managers in charge of information technology or IT Service Delivery Managers within each Organization are responsible for ensuring that devices, systems, and applications under their control are in compliance with the **Network Infrastructure Policy**.
- 7.7. King County departments/agencies are responsible for informing their employees of this policy.